Security for Mobile Computing and Storage Devices

Understanding the Policy and Guidelines

May 2018

Office of Policy and Management

Purpose

As state employees, knowing how to safeguard confidential or restricted data is an important aspect of all our jobs.

The purpose of the Policy on Security for Mobile Computing and Storage Devices is to protect State data that may be stored on mobile devices. In the age of information, it is important that we remain current in knowing how to safeguard the information that is entrusted to us on the public's behalf.

Who is Covered by the Policy?

1. Executive branch employees, whether full or part-time, permanent or non-permanent
2. Executive branch consultants or contracted individuals
3. OPM has extended this policy to: Interns, Summer Workers, Temporary Workers, and Volunteers

Policy's Bottom Line

Confidential or restricted data should not leave the premises of OPM except under certain carefully controlled circumstances – and then it should be safeguarded in every way.

What You Need to Know

1. Identify if you need to have access to any confidential or restricted data on a mobile device.
2. If you do need to have confidential or restricted data on a mobile device, request permission, in writing, using the “Mobile Data Control Form” available on the OPM Intranet.

What You Need to Know

3. If you are authorized to have confidential or restricted data on a mobile device, be sure that the device you are using is “secure”. If in doubt, check with OPM’s Mobile Device Policy Compliance Officer (Jamie Gamble).
4. Do not store or transmit confidential or restricted data on personally owned mobile devices or personally owned computers.
5. Do not transmit confidential or restricted data via E-mail outside of the State network.

What You Need to Know

6. Follow good practices for storing data on secure mobile devices:
   a) Keep only the minimum amount of data necessary to perform the business function.
   b) Store data only for the time needed to perform the business function.
   c) Do not bypass or disable security mechanisms under any circumstances.
7. Remove/delete files as soon as you return to the office and/or are finished using them.

What You Need to Know

Take reasonable and appropriate precautions to protect these devices from unauthorized physical access, tampering, loss or theft.

a) Use “strong” passwords.
b) Log off your computer when temporarily not in use.
c) Do not leave your mobile devices unattended at any time.

What You Need to Know

9. In the event that your mobile device is lost, stolen, misplaced and/or you suspect that there has been unauthorized access, immediately notify your supervisor and/or Division Head. Division Heads will notify MaryAnn Palmarozza. MaryAnn will notify the DAS/BEST Helpdesk if a reasonable potential exists that confidential data may have been stored on the device.
10. If you are unsuccessful in notifying anyone at OPM and a reasonable potential exists that confidential data may have been stored on the device, immediately contact the DAS/BEST Help Desk at (860) 622-2300.

Links to the Details

(Use “TOC” links on the following pages to return here)

Links to the Details

(Use “TOC” links on the following pages to return here)

Definitions of Confidential or Restricted Data

Confidential or restricted data includes but is not limited to **personally identifiable information** that is not in the public domain and if improperly disclosed could be used to:

- ✓Steal an individual's identity;
- ✓Violate the individual's right to privacy; or
- ✓Otherwise harm the individual.

TOC

Definitions of Confidential or Restricted Data

Confidential or restricted data includes but is not limited to **organizational information** that is not in the public domain and if improperly disclosed might:

- ✓Cause a significant or severe degradation in mission capability;
- ✓Result in significant or major damage to organizational assets;
- ✓Result in significant or major financial loss; or
- ✓Result in significant, severe or catastrophic harm to individuals.

TOC

What are some examples of OPM data that is considered confidential or restricted?

- ✓ Personnel information that includes Social Security Numbers
- ✓ Grant Applications that include taxpayer information
- ✓ Long Term Care Database
- ✓ Budget Information
- ✓ Labor Relations Information
- ✓ What else can YOU think of?

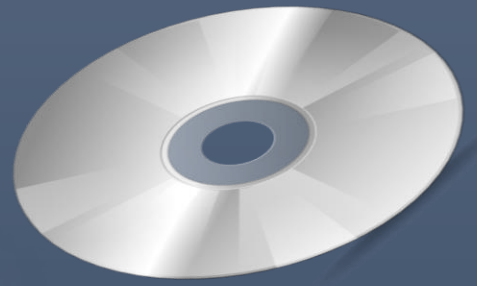
TOC

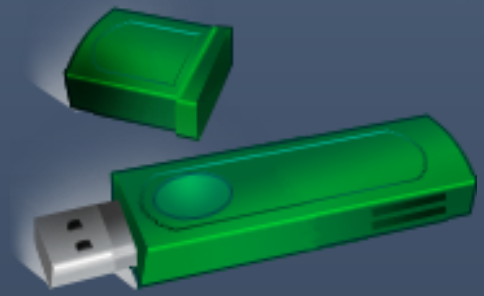
Need Guidance?

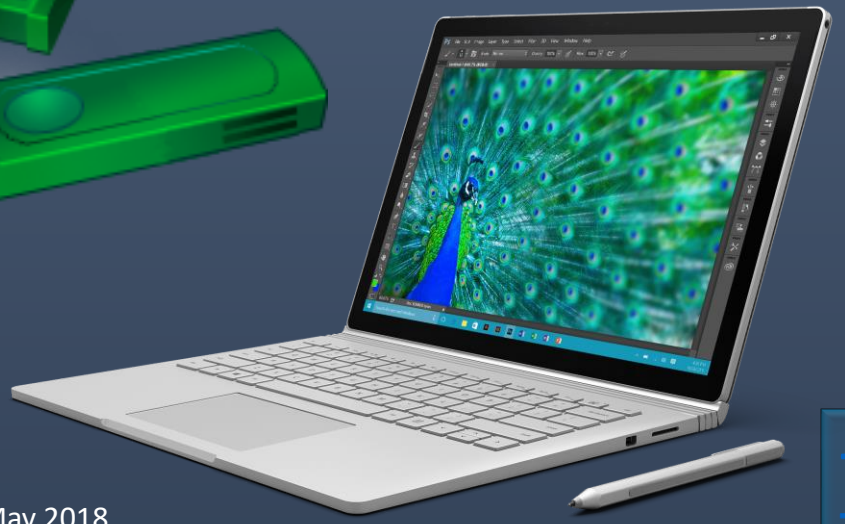
Contact your supervisor and OPM's Mobile Device Policy Compliance Officer (Jamie Gamble) for guidance if you do not know if your data is confidential or restricted.

TOC

What devices are covered by the Policy?







TOC

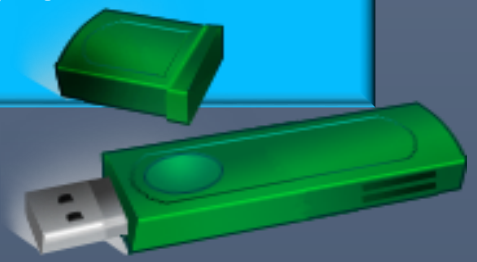
What devices are covered by the Policy?

Mobile **computing** devices include (but are not limited to):

1. Notebooks (Laptops)
2. Tablets
3. iPhones, Droids
4. Cell phones with Internet browsing capabilities

TOC

What devices are covered by the Policy?



Mobile **storage** devices include (but are not limited to):

1. Mobile Computing Devices	5. Thumb Drive (USB keys)
2. Diskettes	6. Jump Drives
3. Magnetic Tapes	7. Compact Discs
4. External/Removable Hard Drives	8. Digital Video Discs

TOC

How to Request Permission to Store Confidential or Restricted Data on a Mobile Device

Complete the “Mobile Data Control Form” available on the OPM Intranet to request permission to store confidential or restricted data on mobile devices. Jamie Gamble, OPM’s Mobile Device Policy Compliance Officer, will coordinate a review and approval by the Secretary of OPM. Once the paperwork is in place you will be given authorization to have the data on your secure mobile device.

TOC

Security Measures for Mobile Devices

A “mobile device” is considered secure when it:

- ✓Has a sufficient level of access control;
- ✓Is protected from malware (i.e., MALicious softWARE designed to destroy, aggravate, wreak havoc, hide potentially incrimination information, and/or disrupt and damage computer systems); and
- ✓Has strong encryption capabilities.

TOC

Use of Personally Owned Mobile Computing and Storage Devices

It is not acceptable to store or transmit confidential or restricted data on personally owned mobile devices or personally owned computers.

TOC

Use of Personally Owned Mobile Computing and Storage Devices

It is not acceptable to connect personally owned hardware or install and/or use non-State licensed software on State of Connecticut systems.

TOC

Use of E-mail to Transmit Confidential or Restricted Data

It is not acceptable to transmit confidential or restricted data via E-mail outside the state system. Data may be transmitted to @ct.gov and @po.state.ct.us e-mail addresses. E-mail transmissions which travel over the Internet or are transmitted from wireless devices, such as an iPhone, are not secure.

TOC

How to Store Confidential or Restricted Data on Secure Mobile Devices

- ✓Encrypt data using methods authorized by BEST.
- ✓Keep the minimum data necessary to perform the business function.
- ✓Store data only for the time needed to perform the business function.
- ✓Protect data from any and all forms of unauthorized access and disclosure.
- ✓Do not bypass or disable security mechanisms under any circumstance.

TOC

Deleting Files

Remove/Delete files from laptops, jump drives and all mobile devices as soon as you return to the office and/or are finished using them!

TOC

Deleting Files

To ensure that your files are completely deleted:

Be sure to empty your recycle bin often or select the file from Windows/Explore and use ***shift-delete*** to delete a file. (Using shift-delete will stop the document from even going into the recycle bin.)

TOC

Deleting files from “My Recent Documents” Folder

To also improve security, remove your recently used documents from the “My Recent Documents” folder:

1. Right-click Start then click Properties. Be sure the Start Menu tab is selected.
2. Click Customize.
3. Click the Advanced tab.
4. Under Recent documents, click Clear List, click OK, and then click OK.

Note that this does not delete the documents from your hard drive.

TOC

How to Protect Mobile Devices from Unauthorized Access: Use Passwords

- ✓Mobile computing devices should have multiple levels of password protected access. Log into the computer with a password and password protect any document that has confidential or restricted data.
- ✓Use only “strong” passwords – a mix of alpha, numeric, special and upper/ lower case characters.
- ✓Do not use any option that “remembers” your password!
- ✓Store passwords, account names, access codes, login instructions, authentication tools separately from mobile devices.

TOC

How to Protect Mobile Devices from Unauthorized Access: Encryption

- ✓Encryption makes data on a mobile device unreadable to anyone who does not have the “key”.
- ✓Mobile devices that have been authorized by the Secretary of OPM to store confidential or restricted data will be encrypted by OPM’s IT staff using BEST approved software.

TOC

How to Protect Mobile Devices from Unauthorized Access: Log Off

All notebooks running Microsoft Windows should be “locked” or secured when temporarily not in use using:

CTRL-ALT-Del (Then select Lock)

or

CTRL-ALT-DEL (Then select Log-off)

TOC

How to Protect Mobile Devices from Being Stolen

- ✓ Do not leave your laptop or any other mobile device unattended in an unprotected area.
- ✓ Do not leave your mobile device in an unlocked vehicle or in plain sight. If it must be left in a car, place it in a locked trunk or cover the device and lock the car doors.
- ✓ Take care when using mobile computing devices in public places, meeting rooms and other unprotected areas to avoid risk of unauthorized persons seeing information visible on the screen.

TOC

Suggestions When Traveling with a Laptop

- ✓ Carry your computer onto a plane in a non-descript carrying case, rather than a distinctive laptop bag, and store under your seat rather than in overhead bins. Do not check it as luggage.
- ✓ Carry confidential or restricted data on a separate mobile storage device (e.g., jump drive or CD) that is packed in a separate carry-on bag.
- ✓ Watch your bags while they are on the scanner belt.

TOC

How to Report a Lost, Stolen or Missing Mobile Device

- You must notify our Agency immediately. Call your immediate supervisor and/or Division Head. You must also leave a message for Jamie Gamble (OPM's Mobile Device Policy Compliance Officer) at 418-6276.
- Divisions Heads will notify MaryAnn Palmarozza (OPM's Chief Administrative Officer). MaryAnn will notify the BEST Helpdesk at (860) 622-2300 if a reasonable potential exists that confidential data may have been stored on the device. The OPM Business Office will process the necessary paperwork.
- If you are unsuccessful in notifying anyone at OPM and a reasonable potential exists that confidential data may have been stored on the device, it is imperative you immediately contact the BEST Help Desk at (860) 622-2300. The BEST Help Desk will begin incident response, assessment and remediation activities.

TOC

Completion Certificate

Print and fill out your Completion Certificate from the link below:

Mobile Device Training Completion Form

Return your signed form to the IT unit (Jamie Gamble) on the 3rd floor.

TOC

Other Forms

- Mobile Data Control Form available at: OPM Mobile Data Control Form (This form is used to request permission to store confidential or restricted data on a secure mobile device)

- Agency Head Approval – Data Storage on Mobile Devices available at: OPM Agency Head Approval Data Storage Mobile Device Form (This form is used by OPM's agency head to grant permission to store confidential or restricted data on a secure mobile device)

TOC

Questions or suggestions?

Contact: Jamie Gamble

x6276

TOC

Learning Objectives

Now that you have completed this online program, you should be able to:

- ✓State the purpose of the State's Security for Mobile Computing and Storage Devices Policy.
- ✓Define what is meant by "confidential data".
- ✓Define what is meant by "restricted data".
- ✓State 4 examples of a "mobile computing device".
- ✓List 4 examples of a "mobile storage device".
- ✓Describe what makes a mobile device "secure".
- ✓Summarize the procedure for requesting authorization to store confidential or restricted data on a secure mobile device.
- ✓Explain what you should do if your equipment is lost or stolen.
- ✓Describe strategies you can employ for protecting your mobile computing and storage devices.

TOC

Sources

Source: September 10, 2007 Press Release (http://www.ct.gov/governorrell/cwp/view.asp?A=2791&Q=394622)

Source: Department of Administrative Services / BEST, *Policy on Security for Mobile Computing and Storage Devices (Version 1.0).* September 10, 2007. (Security for Mobile Computing and Storage Devices)

TOC

Sources

- Source: State of Connecticut Acceptable Use of State Systems Policy, May 2006 (Addendum added November 2006). (Acceptable use of state systems may 2006)

TOC